UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with a certain account maintained at a premises controlled by Google LLC

Case No. 1:22mJ335

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-1

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1030, 371, 1343, 1349, and1956(h)	Unauthorized Access to a Protected Computer, Conspiracy, Wire Fraud, Money Laundering Conspiracy

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s Adam B. Scholtz
Applicant's signature

Adam B. Scholtz, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 8/29/2022

Joi Elizabeth Peake
Judge's signature

City and state: Winston-Salem, North Carolina

Hon. Joi E. Peake, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Adam B. Scholtz, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

I make this affidavit in support of an application for a search warrant for certain information associated with certain accounts stored at a premises controlled by Google, Inc., ("Google"), an electronic service provider and/or a remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

The information to be searched is described in the following paragraphs and in Attachments A-1, A-2, and A-3. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A), to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B.

I am a Special Agent with the Federal Bureau of Investigation (the "FBI") and have been since April 2004. Prior to joining the FBI, I served in the United States Army as an Infantry Officer. I performed those duties for four years. Since joining the FBI, I have completed specialized training in cyber investigations and currently hold professional certifications in cyber security and computer forensics. I also possess an FBI-based certification that allows

me to conduct computer-based forensic examinations. I currently specialize in investigating computer-based crimes.

This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on my training and experience and the facts as set for the in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030 (computer fraud), 1343 (wire fraud), 371 (conspiracy), 1349 (wire fraud conspiracy), and 1956(h) (money laundering conspiracy) (the "Subject Offenses"), including attempt, have been committed by persons whose identities are still under investigation. There is also probable cause to search the information described in Attachments A-1, A-2, and A-3 for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

THE SUBJECT OFFENSES

Among other ways, a violation of 18 U.S.C. § 1030 exists when a person, intentionally and without authorization, accesses a protected computer if the conduct involved interstate or foreign communication.

A violation of 18 U.S.C. § 1343 exists when a person uses interstate wire communications to execute a scheme to defraud or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises that were material and for the purpose of executing the scheme, the

defendant transmitted in interstate or foreign commerce any writings, signs, signals, pictures, or sounds. United States v. Godwin, 272 F.3d 659, 666 (4th Cir. 2001). Conspiring to commit wire fraud – that is, to violate 18 U.S.C. § 1343 – is a federal offense in its own right. See 18 U.S.C. § 1349.

In addition, the federal money laundering statute makes it a crime to conduct financial transactions with the intent to conceal the proceeds of an unlawful activity. See 18 U.S.C. § 1956(a)(1)(B)(i). A person further violates federal law if she conspires to launder money – that is to violate 18 U.S.C. § 1956(a)(1)(B)(i). See 18 U.S.C. § 1956(h).

Finally, it is a federal crime to conspire with someone else to commit an offense made illegal by federal law. See 18 U.S.C. § 371.

JURISDICTION

This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711, 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711 (3)(A)(i).

PROBABLE CAUSE

On March 16, 2022, Victim-1, a resident of Greensboro, North Carolina, received an email from quickbooks@notification.intuit.com. The email stated she was charged $532.14 for a Norton anti-virus subscription. The email

provided the telephone number 866-339-2131 (the "Scam Telephone Number") for her to call. Victim-1 dialed the Scam Telephone Number, and the person on the other end of the phone said they were with Norton and they transferred Victim-1 to someone named "Alan" in accounting.

Alan told Victim-1 was going to credit her account and instructed her to go in front of her computer. When Victim-1 was in front of her computer a window opened and looked to Victim-1 like a DOS screen that she had seen in the past. Alan asked her to enter the amount of $200 into the window. When Victim-1 entered "$200," the amount on the screen changed to $20,000. Victim-1 told Alan the amount was a mistake and Alan said he would try to fix it. He later said he couldn't fix it, and she needed to return the money.

Alan instructed her to open a Binance.com cryptocurrency account, which she did on her computer. When she was opening the account, Alan told her that it was taking too long, and he asked her for her username and password for this account and for any other accounts she used or logged into.

On March 17, 2022, Victim-1 realized Alan still had access to her computer. She said Alan would flash images on her screen to show her account balances with State Employee's Credit Union ("SECU"). The balances looked similar to the account balances she recognized, and he would ask her to check the balances to make sure they were accurate. Victim-1 later realized this was

done to mislead her so she would not notice future wire transfers leaving her account.

On March 18, 2022, Alan told Victim-1 that she needed to send the money she owed Norton in cash. He provided her instructions to send the money via United Parcel Service ("UPS") to an individual named Cordell Thomas at address 117 23rd Street South, Battle Creek, Michigan 49015. Victim-1 was instructed to take pictures of everything she did and to send the pictures to Alan by text message. He instructed her not to declare that there was cash in the package when she shipped it, but rather, to claim the package contained chocolate and clothes. Victim-1 did, in fact, make this shipment and said she was petrified and frightened during this period.

On March 19, 2022, Victim-1 received a text message or an email that notified her the package was delivered. She later received a call from someone named "Sean" from UPS who questioned her about the package and what the contents were. Sean said there would be a further investigation. After she received the phone call from Sean, she called Alan to tell him she had received the call regarding the shipment. Alan said not to worry about it and that he would take care of it.

On March 21, 2022, Alan instructed Victim-1 to open an FTX.us online banking personal account (the "FTX Account") and to send a wire of $50,000. The amount of money was determined because $50,000 was the minimum

amount of money that could be sent via an FTX personal account. When she opened the FTX Account, Alan instructed her by phone on what website to go to by telling her what to type in the internet browser's address bar. FTX required a video recording to open the account. Alan provided Victim-1 with a script for her to read in the video.

Victim-1 made several wire transfers from her SECU account to the FTX Account. Anytime she went to the bank to wire money, Alan or another person, "Kevin," would remotely print a form on her printer to give to the teller. They instructed her to rotate branches and not to go to the same branch. Victim-1 recalled that she went to three different SECU branches during this period. Victim-1 continued to send wires because Alan or Kevin told her the wires were denied. They would print out false account balances to calm her down and to mislead her into thinking her account balances had not changed.

Victim-1 provided consent for the FBI to search her computer and her email account. On April 6, 2022, an FBI Computer Scientist analyzed the initial email Victim-1 received from quickbooks@notification.intuit.com. The email headers contained an "X-Originating-IP" of 167.89.82.160. Whois information reveals this IP belongs to SendGrid, a U.S. company which facilitates mass email campaigns typically for marketing purposes.[1] SendGrid

[1] Whois is a widely-used internet recording listing that identifies the owners of internet domains and provides some contact information for those owners.

may have identifying information for the true sender based on the "Reply-To" email Arikrovel76@outlook.com or the "X-Company" id 9130352725522906. Using SendGrid allowed the sender to place an arbitrary email in the "From" field, while placing a true email they access in the "Reply-To" field so that any replies from victims go to one of the sender's legitimate addresses.

On April 7, 2022, I reviewed a forensic image of Victim-1's laptop hard drive. During the review, the following artifacts were identified:

Date / Time (UTC)[2]	Event
3/16/2022 5:22:04 PM	File system created artifact for "Invoice_1037_from_Norton.pdf"
3/16/2022 5:28:17 PM	Chrome browser history artifact was created for https://nsupport.online
3/16/2022 5:28:52 PM	Chrome browser was used to download the file "support.Client.exe" from https://hide13.xyz
3/16/2022 5:28:52 PM	support.Client.exe file was created on the hard drive
3/16/2022 5:31:15 PM	Chrome browser was used to visit https://forms.gle/LrzgxRUiRp2yLT2aA
3/16/2022 5:31:15 PM	Chrome browser was used to visit https://docs.google.com/forms/d/e/1FAIpQLSfHvVEHgPEC-GEpioiLjIyYcD-SRgX6veaVj4m-2E-K4cZDBA/viewform?usp=send_form

[2] Coordinated Universal Time

A review of the support.Client.exe file by an FBI Computer Scientist identified the file as an endpoint agent for the remote access tool ConnectWise. Once installed on a computer, the program enables the computer to be remotely accessed and controlled based on the computer's user account authority.

The opensource website domaintools.com captured a screenshot of the website nsupport.online on March 1, 2022. Based on the screenshot below,[3] the website purports itself to be a Norton Antivirus support page. Based on my training and experience phishing websites such as nsupport.online are created as part of the scheme in order to elicit a victim's credentials to accounts or services, to download malware, or to redirect web traffic to other websites that serve that function.

[3] https://research.domaintools.com/research/screenshot-history/nsupport.online/#0

Opensource research shows the website https://nsupport.online was hosted on IP address 198.12.84.71, and the website https://hide13.xyz was assigned IP address 198.23.213.36. Both IP addresses were hosted by ColoCrossing, located in Buffalo, New York. ColoCrossing is a virtual server service provider of data center IT services, including dedicated server hosting, data center colocation, and managed services.

Based on the information collected to date, I assess that Victim-1 opened the email with the subject "Invoice_1037_from_Norton.pdf" and then called the number provided in the email. Victim-1 was then directed by the unknown subjects to go to her computer and visit the website for https://nsupport.online where her browser was redirected to https://hide13.xyz and downloaded the executable file support.Client.exe. This executable file installed a ConnectWise agent to Victim-1's computer which provided remote access capabilities enabling the unknown subjects to remotely access and take control of her computer.

ConnectWise is a suite of commercially available programs developed for remote access capabilities. Based on information provided on the ConnectWise support page, the agent can be created and hosted on a server and downloaded. Based on my training and experience, it is my assessment the server located at IP addresses 198.12.84.71 was used to host the fake Norton Antivirus phishing website used to deceive the victim into believing the unknown

subjects were legitimate employees of Norton. The website was likely used to redirect the victim to IP address 198.23.213.36, with the URL https://hide13.xyz, where unidentified subjects used the ConnectWise agent program to establish connections to the victim's computer.

The following wire transfers and cash withdraws were made from Victim-1's SECU account at the direction of Alan or Kevin:

Date	Activity
03/18/2022	$4,0000 Cash Withdraw
03/18/2022	$16,000 Cash Withdraw
03/22/2022	$75,000 Outgoing Wire Transfer
03/22/2022	$80,000 Outgoing Wire Transfer
03/23/2022	$75,000 Outgoing Wire Transfer
03/24/2022	$83,000 Outgoing Wire Transfer
03/25/2022	$19,500 Outgoing Wire Transfer
03/25/2022	$45,000 Outgoing Wire Transfer (Recalled by SECU)
Total	$352,520

On May 11, 2022, the FBI received records from FTX.us obtained by the Greensboro Police Department by a state search warrant. The account was in the name of Victim-1. A review of the deposits into the account were identical to the outgoing wires sent from Victim-1's SECU account. Once the funds were received into the FTX.us account, they were converted to cryptocurrency Tether ("USDT")[4] and then transferred to cyptocurrency wallet,

[4] USDT is the symbol for Tether, a is an asset-backed cryptocurrency stablecoin which is pegged to the value of the Unites States dollar.

0x65380f02A0A54cA0a80A3dB3379C8e4F512ce9B2 ("Wallet-1"), minus the conversion and transaction fees.

Time (UTC)	Coin	Amount	Destination Cryptocurrency Address
03/22/2022 T15:50:51.887303+00:00	USD	80,000	Deposit
03/22/2022 T15:54:47.064707+00:00			Converted from USD to USDT
03/22/2022 T15:55:26.119455+00:00	USDT	79513.02	Wallet-1
03/22/2022 T19:25:47.622425+00:00	USD	75,000	Deposit
03/22/2022 T19:27:46.312113+00:00			Converted from USD to USDT
03/22/2022 T19:30:15.017166+00:00	USDT	74536.02	Wallet-1
03/23/2022 T17:15:43.529758+00:00	USD	75,000	Deposit
03/23/2022 T17:21:52.959902+00:00			Converted from USD to USDT
3/23/2022 T17:29:02.313044+00:00	USDT	74565	Wallet-1
03/24/2022 T21:08:07.724076+00:00	USD	83,000	Deposit
03/24/2022 T21:11:14.524301+00:00			Converted from USD to USDT

Time (UTC)	Coin	Amount	Destination Cryptocurrency Address
03/24/2022 T21:12:34.818275+00:0 0	USDT	82462.63	Wallet-1
03/25/2022 T17:34:04.306116+00:0 0	USD	19,500	Deposit
03/25/2022 T17:37:37.640243+00:0 0			Converted from USD to USDT
03/25/2022 T17:37:58.979755+00:0 0	USDT	19392.88	Wallet-1
03/25/2022 T19:02:24.500521+00:0 0	USD	45,000	Deposit (Recalled by SECU)

Research conducted by the FBI using commercial cryptocurrency analysis tools identified the FTX.us outgoing transactions to Wallet-1 were then transferred to two cryptocurrency wallets maintained by Binance.com:

- 0xe8789a5160568B745F82DaebD0B4EA37Eba299B6 ("Wallet-2")
- 0x9008265003b42f317621999638B37858245bC0EB ("Wallet-3")

On June 2, 2022, I received Binance.com account records obtained by the Greensboro Police Department for the addresses associated with Wallet-2 and Wallet-3.

A review of the Know Your Customer ("KYC") information for address Wallet-2 identified the account holder as Gaurav Pahwa, date of birth May 18,

1991, a citizen of India.[5] Pahwa provided email account gauravpahwa18@gmail.com ("**TARGET GOOGLE ACCOUNT 1**") as his registration email address. Binance.com records identified numerous approved devices associate with Pahwa's account. The following were the last four devices associate with the account:

Device ID:	1653569551807sCKQm6kqDfnNkPDpYts
Identification Type:	FaceID
Login IP:	49.36.191.91
Operator:	Vodafone India
Device_uuid:	D23D8949-7E08-46D8-B9A3-AE4995EA0803
Device Name:	Gaurav's iphone 12pro
Device ID:	1652466599064rfVIk3GXmtmwITWvPvv
Login IP:	49.36.191.43
Platform:	iPad
Webgl Vendor:	Apple Inc.
Device Name:	Chrome V101.0.4951.44 (iOS)
Web_Timezone:	Asia/Calcutta
System Version:	iOS 15.4
Fingerprint:	d5d923233f8666b3400c1dbb1e413b0b
User Agent:	Mozilla/5.0 (iPad; CPU OS 15_4 like Mac OS
Device ID:	1652358157896lztTjTFNbDqrKkA6h9i
Identification Type:	FingerID
Login IP:	49.36.187.181
Operator:	AirTel
Device_uuid:	2B7676BE-9631-4CD3-B649-0F67F326A92E
Device Name:	Gaurav's iPhone SE
Device Custom Name:	Gaurav's iPhone SE
Brand Model:	iPhone SE 2nd Gen

[5] "Know Your Customer" refers to standards adopted by some cryptocurrency exchanges to know the identities of the people who use those exchanges.

Device ID:	1652140365195h4GkFdWcuCnEi8ORs6C
Login IP:	49.36.191.43
Platform:	MacIntel
Webgl Vendor:	Google Inc. (Intel Inc.)
Device Name:	Chrome V100.0.4896.127 (Mac OS)
Web Timezone:	Asia/Calcutta
System Version:	Mac OS 10.15.7
Fingerprint:	8158edaa19eca24bdf83356fbae798d6

A review of the KYC information for address Wallet-3 identified the account holder as Rupa Kumari Chaudhary, date of birth November 16, 1996, a citizen of India. Chaudhary provided email address rupachaudhary1611@gmail.com ("**TARGET GOOGLE ACCOUNT 2**") as her registration email address and telephone number +918961199605. Binance.com records also identified the Chaudhary's approved device was an iPhone with FaceID as an identification method. The following device was approved to interact with the account:

Device ID:	1652286680998N1jY6zvduWs4wIRfA6W
Identification Type:	FaceID
Login IP:	152.57.99.14
Operator:	Jio
Device_uuid:	93596E26-DA37-4DF2-A069-DEB32E635A11
Device Name:	iPhone
System Version:	15.4.1
Device Custom Name:	iPhone
Brand Model:	iPhone13,3

In my training and experience, Apple generally requires users establish accounts with that company in order to use Apple devices, including iPhones, and iPads. In my training and experience, iPhone users commonly establish a user account with Apple to download applications and use Apple services such as iTunes, iCloud and iMessage. Therefore, based on my training and experience and the information described above, I expect there are Apple accounts associated with the individuals and email addresses listed on TARGET GOOGLE ACCOUNT 1 and TARGET GOOGLE ACCOUNT 2.

On March 7, 2022, Victim-2, a resident of Houston, Texas, received an email from quickbooks@notification.intuit.com regarding a Norton subscription that he did not use. The email had an attachment with an invoiced and advised his balance was for over $500.00. Victim-2 called the number on the email, the Scam Telephone Number, to try to get his money back. Victim-2 followed the instruction of the employee on the phone ("Unidentified Subject-1") and went to the nsupport.online website, which appeared to Victim-2 to be a legitimate Norton website. The Unidentified Subject-1 asked him to enter into his computer the refund amount. The amount he entered was somehow changed to a higher amount. The Unidentified Subject-1 told him that he owed the excess money to Norton. Victim-2 then noticed the Unidentified Subject-1 could control his computer.

Victim-2 checked his Chase bank account and could see there was extra money in his account. He sent several wires to try to return the money at the direction of the Unidentified Subject-1. Victim-2 didn't realize the money had actually been transferred from his niece's account which was linked to his. He sent $79,600 of her money which Unidentified Subject-1 had moved into his account after gaining access to his bank account.

In addition to the Scam Telephone Number, VICTIM-2 communicated with Unidentified Subject-1 by phone at 530-322-9672 and 724-517-3477. Victim-2 sent me the email from Norton. A review of the email header information identified the sender of the email used the SendGrid service and with the Reply-To address as tasidoklam15@gmail.com ("**TARGET GOOGLE ACCOUNT 3**").

A review of Victim-2's bank account statement Chase Bank wire transfer information. The following wire transfers were conducted at the direction of the Unidentified Subject-1.

Date	Activity
03/07/2022	$53,700 - Outgoing Wire Transfer Recipient: Veronica Hidalgo Recipient Bank: Banco Internacional Del Peru Account: 2473285998932
03/08/2022	$25,900 Outgoing Wire Transfer Recipient: Wuilkerman Carvajal Recipient Bank: Banco Internacional Del Peru Account: 1433286167714
Total	$79,600

Subscriber records obtained from Google by federal grand jury subpoena for TARGET GOOGLE ACCOUNT 3 was established in the name of Tasid Oklam (Google Account ID: 154902526114) and was created on February 2, 2022.

BACKGROUND REGARDING ONLINE SCAMS

In my training and experience, I have learned that online scams are commonly conducted by a group of individuals with specific roles and responsibilities. One individual may be responsible for obtaining unauthorized access to computers and online accounts, another individual may recruit co-conspirators to open bank accounts, and other individuals launder the illicit proceeds and transfer money to co-conspirators. Because the co-conspirators may not be located in the same geographic area, the conspiracy requires communication conducted over voice calls, text messages, email and/or private messaging applications such as iMessage, WhatsApp, Telegram, or Google Hangouts.

In my training and experience, individuals involved in online scams often create online communication accounts in fictitious names in order to facilitate the scheme and to hide their true identity.

INFORMATION MAINTAINED BY GOOGLE

In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access to the

public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account(s) listed in Attachments A-1, A-2, and A-3. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computer of Google are likely to contain stored electronic communications (including retrieved and retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

In my training and experience, email service providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers,

alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may contain evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provides substantial evidence as to their identity, location or illicit activities.

In my training and experience, email service providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website) and other log files that reflect usage of the account. In addition, email service providers often have records of the internet protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must us an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquires, or complaints from other users. Email service providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, when, where, why, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the fore going, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email service provider can show how and when

the account was accessed or used. For example, as described below, email service providers typically log the IP addresses from which users access the email account along with the time and dates. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and the use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

Google also offers applications that allow users to communicate with each other through instant messaging and voice communications. They also provide other services, such as calendar services, storage of browsing history, locations history, and tools related to the administration of user created websites. In my training and experience, information from these other services

may constitute evidence of the crimes under investigation because, for example, the information can be used to identify the account's user or users.

Google provides a service through which the computer user can search web pages for text that the user types in, and under some circumstances, Google saves the user's text searches for later retrieval. Google may also keep records of the webpages or IP addresses that a user clicks on or types directly into his web browser's address bar (as opposed to Google's search bar), if the user is using Google's web browser (Google "Chrome") and has logged into Google Chrome with his Google account's username and password.

Google uses different names to identify the many services it offers. These include: Account Activity, Chrome, Gmail, Google Calendar, Google Cloud Platform, Google Docs, Google Drive, Google Maps, Google+, Google Hangouts, Google Voice, Google Talk, Google Wallet, Google Allo, Google Duo, Google Photos, Web Search, Web History, Location History, YouTube, and iGoogle.

CONCLUSION

Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR NON-DISCLOSURE

I further request that pursuant to the preclusion of notice provisions of 18 U.S.C § 2705(b), Google be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for one year from the date of the warrant. Such an order is justified because notification of the existence of this warrant would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber(s) an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Much of the expected evidence in this case is electronic and may be subject to deletion or destruction. Additionally, the subject(s) of the investigation may reside abroad, and earlier notification may allow them to flee jurisdictions that will not extradite them to the United States.

WHEREFORE, it is respectfully requested that the Court grant the attached Order directing Google not to disclose the existence of the warrant or the application except to the extent necessary to carry out the Order.

Respectfully submitted,

/s Adam B. Scholtz
Adam B. Scholtz
Special Agent
Federal Bureau of Investigation

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.

August 29, 2022

The Hon. Joi E. Peake
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A-1

Property to be Searched

This warrant applies to information associated with the following Google Account that are stored at premises controlled by Google, LLC, an electronic service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California (collectively with the accounts described in Attachments A-2 and A-3, the "TARGET GOOGLE ACCOUNTS"):

- **TARGET GOOGLE ACCOUNT 1:** gauravpahwa18@gmail.com

ATTACHMENT A-2

Property to be Searched

This warrant applies to information associated with the following Google Account that are stored at premises controlled by Google, LLC, an electronic service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California (collectively with the accounts described in Attachments A-1 and A-3, the "TARGET GOOGLE ACCOUNTS"):

- **TARGET GOOGLE ACCOUNT 2**: rupachaudhary1611@gmail.com

ATTACHMENT A-3

Property to be Searched

This warrant applies to information associated with the following Google Account that are stored at premises controlled by Google, LLC, an electronic service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California (collectively with the accounts described in Attachments A-1 and A-2, the "TARGET GOOGLE ACCOUNTS"):

- **TARGET GOOGLE ACCOUNT 3**: tasidoklam15@gmail.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachments A-1, A-2, and A-3 is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information from Account inception to present to the government for each account listed in Attachments A-1, A-2, and A-3:

a. The contents of all emails associated with the TARGET GOOGLE ACCOUNTS, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. The contents of all communications associated with the TARGET GOOGLE ACCOUNTS;

c. All records or other subscriber information, in any form kept, regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the TARGET ACCOUNTS, login IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, subscriber change history, and means and source of payment (including any credit or bank account number), detailed billing records, and the types of service utilized;

d. All records or other information stored at any time by any individual using the TARGET GOOGLE ACCOUNTS, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records relating to the location from which the TARGET GOOGLE ACCOUNTS was accessed;

f. All records pertaining to devices associated with the TARGET GOOGLE ACCOUNTS to include serial numbers, model type/number, IMEI, phone numbers, MAC Addresses, Android IDs and FCC ID numbers;

g. All records pertaining to communications between the Provider and any person regarding the TARGET GOOGLE ACCOUNTS, including contacts with support services and records of actions taken;

h. All records or other subscriber information as described in section I.c for any and all accounts linked by creation email address, recovery email address, forwarding/fetching email address, and telephone number(s) associated; and

i. All records of subscriber change history associated with the TARGET ACCOUNTS, including, but not limited to, changes to the password, recovery email, and telephone number for the TARGET ACCOUNTS.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 1030 (Computer Fraud), 1343 (Wire Fraud), 371 (Conspiracy), 1349 (Wire Fraud Conspiracy), and 1956(h) (Money Laundering Conspiracy) ("SUBJECT OFFENSES"), those violations involving the TARGET GOOGLE ACCOUNTS, as follows:

a. Evidence indicating how, when and where the TARGET GOOGLE ACCOUNTS were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the SUBJECT OFFENSES and to the TARGET GOOGLE ACCOUNTS user(s) or owner(s);

b. The identity of the person(s) who created, used, or controlled the TARGET GOOGLE ACCOUNTS, including records that help reveal the geo-location, travel, and whereabouts of such person(s);

c. Evidence referencing or revealing the unauthorized access of computers and other electronic devices;

d. Evidence referencing or revealing the creation and use of spoofed online accounts, including email and VOIP accounts;

e. Evidence referencing or revealing online scams including scripts to defraud victims, communications with victims, and efforts to facilitate access to victim information;

f. Evidence referencing or revealing the use of Virtual Private Networks and other IP masking services, including ConnectWise;

g. Evidence referencing or revealing the transfer of money through financial institutions, cryptocurrency exchanges, or other money transfer services;

h. Evidence referencing or revealing possible victims of fraud or computer intrusions, including individuals, companies, government entities, or other organizations, and information

concerning the potential victims, including names, personal identifiable information, accounts, contracts, invoices, communications, and any other information that could be used in furtherance of the SUBJECT OFFENSES;

i. IP logs, geo-locational information or other records that will help establish computers and electronic devices used to access the TARGET GOOGLE ACCOUNTS and the location of those devices; and

j. Communications between and/or regarding user(s) of the TARGET GOOGLE ACCOUNTS and any other person or persons involved in the SUBJECT OFFENSES.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.